IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s)	Timothy J. COLLINS et al.
Application No.	10/650,153
Filing Date	August 26, 2003
Title	METHOD, APPARATUS, AND SYSTEM FOR DETERMINING A FRAUDULENT ITEM
Examiner	Charles C. Agwumezie
Art Unit	3685
Conf. No.	7078

Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
Via EFS-Web

APPEAL BRIEF

Appellant respectfully appeals from the Final Office Action dated December 23, 2010 and the supplemental Final Office Action dated June 17, 2011 in which Claims 1, 5, 6, 8, 11, and 19-29 were rejected. The Notice of Appeal and associated fees were filed on April 18, 2011 along with an Amendment canceling Claims 30-33. The fees associated with the Appeal Brief accompany this paper. Thus, this Appeal Brief is timely filed.

REAL PARTY IN INTEREST

This application is assigned to Motorola Solutions, Inc. of Schaumburg, IL.

RELATED APPEALS AND INTERFERENCES

No related appeals or interferences are pending.

STATUS OF CLAIMS

Pending:	Claims 1, 5, 6, 8, 11, and 19-29 are pending
Rejected:	Claims 1, 5, 6, 8, 11, and 19-29 are rejected
Canceled:	Claims 2-4, 7, 9, 12-18, and 30-33 have been previously canceled.
Objected to:	None
Withdrawn:	None
Appealed:	Claims 1, 5, 6, 8, 11, and 19-29

STATUS OF AMENDMENTS

An Amendment and Response to Final Office Action was submitted on April 18, 2011 concurrently with the Notice of Appeal. This Amendment canceled Claims 30-33. In the Final Office Action, Claims 30-33 were rejected under 35 U.S.C. §112, first paragraph, as failing to comply with the written description requirement. Based on the cancellation of these Claims, Appellant is not appealing this rejection.

On June 17, 2011, Examiner issued a supplemental Final Office Action entering the amendment submitted on April 18, 2011 to cancel Claims 30-33. Appellant is appealing the §101 and §103 Rejections in the supplemental Final Office Action of June 17, 2011.

SUMMARY OF CLAIMED SUBJECT MATTER

1. A method for determining if an item is a fraudulent item, the method comprising the steps of:	Abstract
obtaining by radio means a first number from an RFID tag associated with the item or item's packaging;	Radio means includes the RF tag reader 702 in FIG. 7 and the RF reader 802 in FIG. 8 FIG. 6, elements 601 and 603 p. 6, lines 1-4; the first number being the numbers existing on the identification tag
electronically reading a second number printed on the item or packaging of the item;	FIG. 6, element 605 p. 6, lines 12-17; the signature being the second number
utilizing a public-key cryptographic process and contents of the RFID tag to cryptographically decide whether the second number is a public-key signature of the first number; and	FIG. 6, element 607 p. 6, lines 17-28
determining authenticity of the item based on the result of the decision.	FIG. 6, element 611, p. 6 lines 17-27

5. The method of claim 1 wherein the step of determining the item's authenticity comprises associating the item with an authentic item if the signature is verified, otherwise associating the item with a forged item.	FIG. 6, element 611, p. 6 lines 17-27

6. A method of manufacturing a product in order to prevent forgery, the method comprising the steps of:	FIG. 5
programming an anti-forgery RFID tag, pre-programmed with an unalterable first number, with a second number, the unalterable first number probabilistically rarely the same number as unalterable first numbers in other anti-forgery RFID tags;	FIG. 5, elements 501, 502, 503 p. 5, lines 12-21 p. 2, lines 13-24
determining a third number that is a cryptographic signature over the first and second numbers;	FIG. 5, element 505 p. 5, lines 22-24 p. 2, lines 18-21

affixing the anti-forgery RFID tag comprising the first and second numbers to either the product or packaging associated with the product; and	FIG. 5, element 507 p. 5, lines 26-32
affixing the third number to either the product or the packaging associated with the product.	FIG. 5, element 507 p. 5, lines 26-32

8. The method of claim 6 wherein the step of affixing the third number to either the product or the packaging associated with the product comprises the step of printing the third number on the product or the product's packaging.	FIG. 5, element 507 p. 5, lines 26-32

11. A method comprising the steps of:	
obtaining an RFID tag comprising a first number;	FIG. 5, elements 501, 502, 503 p. 5, lines 12-21 the first number being both numbers from the RFID tag
utilizing a private key and the first number to create a second number that is a cryptographic signature, such that cryptographic verification of the second number insures authenticity of an item; and	FIG. 5, element 505 p. 5, lines 22-24 the second number being the digital signature
affixing the second number and the RFID tag to the item or packaging.	FIG. 5, element 507 p. 5, lines 26-32

19. The method according to claim 1 wherein a bar code is used for rendering the second number that is printed on the item or item's packaging.	FIG. 1, element 102 p. 3, lines 17-18

20. The method according to claim 11, wherein a bar code is used for rendering the second number that is affixed on the item or item's packaging.	FIG. 1, element 102 p. 3, lines 17-18

21. A method for determining if an item is a fraudulent item, the method comprising the steps of:	Abstract
obtaining by radio means a first and second number from an RFID tag, wherein the first number is unalterable and unique or semi-unique and the second number is associated with the item;	Radio means includes the RF tag reader 702 in FIG. 7 and the RF reader 802 in FIG. 8 FIG. 6, elements 601 and 603 p. 6, lines 1-4 FIG. 5, elements 501, 502, 503 p. 5, lines 12-21
electronically reading a third number;	FIG. 6, element 605 p. 6, lines 12-17; the signature being the third number
utilizing a public-key cryptographic process and the first and second numbers to cryptographically decide whether the third number is a public-key signature of a combination of the first and second numbers; and	FIG. 6, element 607 p. 6, lines 20-21
determining authenticity of the item based on the result of the decision.	FIG. 6, element 611 p. 6, lines 23-28 p. 5, lines 22-24

22. The method according to claim 21 further comprising the step of electronically determining whether the RFID tag is an anti-forgery RFID tag.	FIG. 6, element 604 p. 6, lines 8-11

23. The method according to claim 21, further comprising electronically determining whether a specific physical feature or a behavioral feature of the RFID tag matches that of an anti-forgery RFID tag.	FIG. 6, element 604 p. 6, lines 4-11

24. The method according to claim 21 further comprising the step of verifying that the second number is associated with the item.	FIG. 2, element 202 p. 7, lines 11-14 p. 3, line 32 – p. 4, line 1

25. The method according to claim 24, wherein the verification is performed electronically using an optical scanner.	FIG. 7, element 703 p. 6, line 15

26. The method according to claim 21 further comprising the step of electronically determining whether the second number is an Electronic Product Code (EPC) of the item.	p. 4, line 2-5

27. The method according to claim 21, wherein the reading is performed by a bar code scanner.	FIG. 7, element 703 p. 6, line 15

28. A method according to claim 6, wherein the second number is associated with the product.	p. 3, line 32 – p. 4, line 5

29. A method according to claim 1, wherein:	
the first number contains a third and fourth number,	FIG. 3 the first number being the numbers existing on the identification tag p. 4, lines 4-5
the third number is concatenated with, and contains different information than, the fourth number,	p. 3, line 22 – p. 4, line 5
the third number includes product information of the item,	p. 4, lines 4-5
the public-key cryptographic process is used with the third and fourth numbers, and	FIG. 5, element 505 p. 5, lines 22-24
only if the public-key cryptographic process cryptographically decides that the second number is a public-key signature of the third and fourth numbers is the product determined to be authentic.	FIG. 6, element 607 p. 6, lines 15-21

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1) Claims 1, 5-6, 8, 11, and 19-29 are rejected under 35 U.S.C. §101 because the claimed invention is directed to non-statutory subject matter.
2) Claims 1, 5-6, 8, 11, 19-25, 27-28, and 31-33 are rejected under 35 U.S.C. §103(a) as being unpatentable over Kay (US 6,223,166) in view of Halperin et al. (US 6,226,619, hereinafter Halperin).
3) Claims 26 and 29-30 are rejected under 35 U.S.C. §103(a) as being unpatentable over Kay (US 6,223,166) in view of Halperin et al. (US 6,226,619, hereinafter Halperin) as applied to Claim 21 above, and further in view of Coopersmith et al. (US 6,069,955, hereinafter Coopersmith).

ARGUMENT

1) **Claims 1, 5-6, 8, 11, and 19-33 are rejected under 35 U.S.C. §101 because the claimed invention is directed to non-statutory subject matter.**

With respect to independent Claims 1, 6, 11, and 21, Appellant respectfully submits that Examiner is in error in holding these Claims and their associated dependent Claims as being directed to non-statutory subject matter. Appellant respectfully submits that each of these Claims explicitly passes the Machine-or-Transformation Test.

In particular, Claim 1 recites radio means and an RFID tag associated with an item. Claim 6 recites an anti-forgery RFID tag and a product or packaging to which the anti-forgery RFID tag is affixed. Claim 11 recites an RFID tag affixed to an item. Finally, Claim 21 recites an RFID tag and an item. Accordingly, Appellant respectfully submits that the §101 Rejection is in error as each of these independent method claims is tied to an RFID tag and an associated item.

Examiner has held in the Final Office Action on pages 2-3 that:

> In response Examiner asserts that none of the claims specifically states the machine which carries out the obtaining and/or the reading. For example a recitation of a specific machine in the preamble is insufficient to overcome 101 rejection. Likewise it is insufficient to recite machine activity in some steps and not others. In each case it amounts to extra solution activity. If this is not the case then where do we draw the line for overcoming the 101 rejection? Accordingly it is Examiner's position that the claimed invention is directed to non-statutory subject matter because of lack of consistency in machine activity recitation. (Final Office Action, 6/17/2011, page 2, last paragraph).

First, Examiner seems to be concerned about what machine carries out the obtaining and/or reading. Appellant respectfully submits that the obtaining and/or reading steps pertain to an RFID tag, which clearly is a machine. One of ordinary skill in the art would clearly recognize that such reading is being performed by an RFID reader.

Examiner's position, that the claimed invention is directed to non-statutory subject matter because of lack of consistency in machine activity recitation, is not a legal basis for holding the Claims as not being statutory subject matter. Examiner states "Likewise it is insufficient to recite machine activity in some steps and not others. In each case it amounts to extra solution activity. If this is not the case then where do we draw the line for overcoming the 101 rejection?" In response to Examiner's question, Appellant has reviewed the July 27, 2010 Interim Guidance for Determining Subject Matter Eligibility for Process Claims in View of *Bikski v. Kappos* (available online at www.uspto.gov/patents/law/exam/bilski_guidance_27jul2010.pdf). Appellant finds no such guidance that a statutory claimed method must recite a machine in every step.

Rather, this Interim Guidance looks to whether the recitation of a machine is particular, meaningful, practical, tangible, etc. (Interim Guidance, p. 1, Factors Weighing Toward and Against Eligibility). This Guidance does suggest that a machine implementing the steps is one factor, but not the only factor as suggested by the Examiner. Appellant respectfully submits that the factors associated with the independent Claims 1, 6, 11, and 21 weigh heavily in favor of eligibility.

Further, Examiner suggests that Claims 1, 6, 11, and 21 fail the machine prong because the "tie" is representative of extra-solution and/or not tied to any particular machine or apparatus. Clearly, an RFID tag is a particular machine or apparatus as is the associated item to which the tag is affixed. Appellant respectfully submits that the inquiry needs to go no further. Claims 1, 6, 11, and 21 are methods tied to a particular machine or apparatus, i.e. the RFID tag and associated item to which the tag is affixed. Based on a thorough reading of this Interim Guidance, Appellant respectfully notes these factors are to be considered when analyzing the claim as a whole to evaluate whether a method claim is directed to an abstract idea. Clearly Claims 1, 6, 11, and 21 are directed to RFID tags, which is not an abstract idea. Appellant respectfully submits that based on this guidance, Claims 1, 6, 11, and 21 are clearly directed to statutory subject matter.

Additionally, Appellant respectfully submits that no Court has held that each and every step in a method claim must recite an explicit machine or transformation. Rather, the current precedent based on *Bikski v. Kappos* has been to examine method claims on the whole rather than step by step. As recently noted by the Federal Circuit, "[I]nventions with specific applications or improvements to technologies in the marketplace are not likely to be so abstract that they override the statutory language and framework of the Patent Act." *Research Corp. Technologies, Inc. v. Microsoft Corp.,* 627 F.3d 859, 869 (Fed. Cir. 2010). Clearly, Appellant's invention is a specific application of RFID for forgery detection.

Accordingly, Appellant respectfully requests withdrawal of this rejection.

2) Claims 1, 5-6, 8, 11, 19-25, 27-28, and 31-33 are rejected under 35 U.S.C. §103(a) as being unpatentable over Kay (US 6,223,166) in view of Halperin et al. (US 6,226,619, hereinafter Halperin).

Kay teaches a cryptographic encoded, ticket issuing and collection system for real-time purchase of tickets by purchasers at remote user stations in an information network that includes a plurality of remote user stations coupled to a server in an information network (Kay, Abstract). The ticket includes a bar code with information stored therein (Kay, Col. 5, lines 40-42). To verify the ticket, the ticket is scanned and decoded using an asymmetric key (Kay, Col. 5, 49-52). Additionally, Examiner states that Kay does not disclose an RFID tag, and relies upon Halperin to teach using an RFID tag (Final Office Action, p. 11).

Appellant's independent Claims 1 and 21 relate to a method for determining an item is a fraudulent item. For example, Claims 1 and 21 include, *inter alia*, reading a first number from an RFID tag on an item, scanning a second number electronically on an item, and determining authenticity of the item if the second number is a public-key signature of the first number. Appellant's independent Claims 6 and 11 relate to a method for manufacturing an RFID tag in order to prevent forgery. For example, Claims 6 and 11

include, *inter alia*, obtaining an RFID tag with a preprogrammed first number, utilizing the first number and a private key to create a second number that is a cryptographic signature of the first number, and affixing the second number and the RFID tag to an item.

Independent Claims 1 and 11

With respect to independent Claims 1 and 11 and their associated dependent Claims, Examiner cites Kay as follows on pages 9-10 of the Final Office Action.

> obtaining a first number associated with the item or item's packaging **(see col. 4, lines 40-60, which discloses scanning a ticket 31 including a bar code 33 representing cipher code definitive of the ticket information in an asymmetric cryptographic system);**
>
> electronically reading a second number printed on the item or packaging of the item **(see col. 4, lines 15-25, which discloses a digital signature may be included in the ticket. The digital signature is created by the seller recording a message in the ticket using his private key);**
>
> utilizing a public-key cryptographic process and contents of the RFID tag to cryptographically decide whether the second number is a public key signature of the first number **(col. 4, lines 40-60, which discloses that a processor 39 receives an output from the receiver 37 and checks the bar code against an asymmetric key stored in a memory 40 and assigned to the event by the seller. Using an asymmetric key assigned by the seller to the event, the bar code is decoded and compared against an event description stored in the memory 40);**

Thus, for Appellant's first number, Examiner cites Kay's barcode representing a cipher code, and for Appellant's second number, Examiner cites Kay's digital signature. Appellant respectfully traverses this rejection as set forth herein.

First, Appellant recites an obtaining via radio means step and an electronically reading step for the first number and the second number, respectively. Specifically, independent Claims 1 and 11 recite separate steps for obtaining the first number and the second number. Kay, on the other hand, merely teaches a single step to read the ticket information (Kay, Col. 4, lines 40-60).

Appellant agrees that Kay teaches the cipher code in Col. 4, lines 40-60, which Examiner cites as Appellant's first number. Appellant further agrees that Kay teaches the digital

signature in Col. 4, lines 15-25, which Examiner cites as Appellant's second number. However, a thorough reading of Kay shows that Kay does not obtain the cipher code and the digital signature in separate steps as claimed by Appellant in Claims 1 and 11. Rather, Kay merely teaches a single step to obtain the ticket information through scanning the ticket (Kay, Col. 4, lines 40-60). Since Kay obtains the ticket information which includes the cipher code and the digital signature in a single scanning step, Appellant respectfully submits that these are not separate numbers, i.e. the first number and the second number, and these are not obtained via separate steps and means. Appellant explicitly obtains the first number via radio means and the second number by electronically reading. That is, Appellant recites separate steps to obtain these numbers in a separate fashion whereas Kay merely obtains barcode information in one step.

Furthermore, assuming the cipher code in Kay represents Appellant's first number and the digital signature in Kay represents Appellant's second number, this is problematic with respect to Appellant's utilizing a public-key cryptographic process step. In particular, Appellant explicitly claims "utilizing a public-key cryptographic process and contents of the RFID tag to cryptographically decide whether the second number is a public key signature of the first number." That is, Appellant is using the first number and the second number in this step. Here, Examiner introduces yet another number from Kay, the asymmetric key assigned by the seller to the event to decode the bar code. Examiner states in the rejection "Using an asymmetric key assigned by the seller to the event, the bar code is decoded and compared against an event description stored in the memory 40." Specifically, Kay fails to teach or fairly suggest deciding whether the second number is a public key signature of the first number.

On pages 4 in the Response to Arguments Section of the supplemental Final Office Action, Examiner states:

> In response Examiner respectfully disagrees and submits that Kay discloses a different number obtained via the memory means. This is because in Kay the second number is electronically read from the ticket - the printed number on the ticket obtained by optically scanning the number. The first number is obtained from the memory of the portable terminal which is compared with the second number in

> order to ascertain the authenticity of the ticket. Accordingly it is Examiner's position that Kay discloses the claimed first and second number.

Importantly, this Response from Examiner cites different numbers from Kay for Appellant's first number and second number from the rejection discussed above. As stated by Examiner, the second number is electronically read from the ticket and the first number is obtained from the memory of the portable terminal.

However, Claims 1 and 11 recite "obtaining by radio means a first number from an RFID tag associated with the item or item's packaging." Thus, Appellant's first number is not stored in the memory of the portable terminal. Rather, it is stored in an RFID tag associated with the item or item's packaging.

In summary, Appellant respectfully submits that the first number and the second number are separately stored and separately obtained from the item, and Appellant cryptographically decides whether the second number is a public key signature of the first number. Kay, in contrast, has one number in a bar code on the ticket. There is another key stored on a portable terminal, and Kay utilizes a single step to read the one number in the bar code.

Based on the foregoing, Appellant respectfully requests reversal of this rejection with respect to independent Claims 1 and 11 and their associated dependent Claims.

Independent Claim 6

The arguments present above with respect to Claims 1 and 11 apply with equal force here. In particular with respect to Claim 6 and its associated dependent Claims, Appellant recites the following steps with the corresponding rejection based on Kay from pages 11-12 of the Final Office Action.

> affixing the anti-forgery RFID tag comprising first and second numbers to either the product or the packaging associated with the product **(see col. 4, lines 15-25, which discloses a digital signature may be included in the ticket)**; and

affixing the third number to either the product or the packaging associated with the product to either the product or the packaging associated with the product **(see col. 4, lines 15-25, which discloses a digital signature may be included in the ticket)**.

Again, Appellant is reciting two separate, independent steps to affix the first and second numbers to the product and to affix the third number to the product. As clearly shown above, Kay merely has a barcode with information printed thereon. Thus, it is not possible for Kay to read on two separate, independent affixing steps.

Examiner merely cites the same section (Col. 4, lines 15-25) where the digital signature may be including in the ticket. Kay teaches including this in the ticket in the barcode. Thus, Kay does not teach these separate steps.

Independent Claim 21

The arguments present above with respect to Claims 1 and 11 apply with equal force here. In particular with respect to Claim 21 and its associated dependent Claims, Appellant recites the following steps with the corresponding rejection based on Kay from pages 13-14 of the Final Office Action.

obtaining a first and second number from an RFID tag, wherein the first number is unalterable and unique or semi-unique and the second number is associated with the item **(see col. 4, lines 40-60, which discloses scanning a ticket 31 including a bar code 33 representing cipher code definitive of the ticket information in an asymmetric cryptographic system);**

electronically reading a third number **(col. 4, lines 40-60, which discloses that a processor 39 receives an output from the receiver 37 and checks the bar code against an asymmetric key stored in a memory 40 and assigned to the event by the seller. Using an asymmetric key assigned by the seller to the event, the bar code is decoded and compared against an event description stored in the memory 40; see col. 4, line 60 - col. 5, line 15)**;);

utilizing a public-key cryptographic process and the first and second numbers to cryptographically decide whether the third number is a public-key signature of a combination of the first and second numbers **(see col. 4, lines 15-25, which discloses a digital signature may be included in the ticket. The digital signature is created by the seller recording a message in the ticket using his private key)**

These steps are similar to Claim 1. However, Examiner here cites the cipher code as the first and second number and the asymmetric key as the third number. As noted above, the asymmetric key in Kay is stored in memory of the portable terminal. Appellant's electronically reading is described as reading the third number from the item.

Based on the foregoing, Appellant respectfully requests reversal of this rejection.

3) **Claims 26 and 29-30 are rejected under 35 U.S.C. §103(a) as being unpatentable over Kay (US 6,223,166) in view of Halperin et al. (US 6,226,619, hereinafter Halperin) as applied to Claim 21 above, and further in view of Coopersmith et al. (US 6,069,955, hereinafter Coopersmith).**

The arguments presented herein with respect to the independent Claims apply here with equal force. Thus, Appellant respectfully requests reversal of this rejection.

SUMMARY

For the reasons presented above, Appellant respectfully believes that all claims under appeal are novel and non-obvious over the art, and respectfully request that the outstanding rejections under 35 U.S.C. §101 and 35 U.S.C. §103(a) be reversed by the Board.

Respectfully submitted,

Date: June 20, 2011

/Lawrence A. Baratta, Jr./
Lawrence A. Baratta, Jr.
Registration No.: 59,553

Attorney for Appellant

CLEMENTS BERNARD
1901 Roxborough Road, Suite 250
Charlotte, NC 28211 USA
Telephone: 704.790.3600
Facsimile: 704.366.9744
lbaratta@worldpatents.com

CLAIMS APPENDIX

The Claims on appeal appear as follows:

1. A method for determining if an item is a fraudulent item, the method comprising the steps of:

obtaining by radio means a first number from an RFID tag associated with the item or item's packaging;

electronically reading a second number printed on the item or packaging of the item;

utilizing a public-key cryptographic process and contents of the RFID tag to cryptographically decide whether the second number is a public-key signature of the first number; and

determining authenticity of the item based on the result of the decision.

5. The method of claim 1 wherein the step of determining the item's authenticity comprises associating the item with an authentic item if the signature is verified, otherwise associating the item with a forged item.

6. A method of manufacturing a product in order to prevent forgery, the method comprising the steps of:

programming an anti-forgery RFID tag, pre-programmed with an unalterable first number, with a second number, the unalterable first number probabilistically rarely the same number as unalterable first numbers in other anti-forgery RFID tags;

determining a third number that is a cryptographic signature over the first and second numbers;

affixing the anti-forgery RFID tag comprising the first and second numbers to either the product or packaging associated with the product; and

affixing the third number to either the product or the packaging associated with the product.

8. The method of claim 6 wherein the step of affixing the third number to either the product or the packaging associated with the product comprises the step of printing the third number on the product or the product's packaging.

11. A method comprising the steps of:

obtaining an RFID tag comprising a first number;

utilizing a private key and the first number to create a second number that is a cryptographic signature, such that cryptographic verification of the second number insures authenticity of an item; and

affixing the second number and the RFID tag to the item or packaging.

19. The method according to claim 1 wherein a bar code is used for rendering the second number that is printed on the item or item's packaging.

20. The method according to claim 11, wherein a bar code is used for rendering the second number that is affixed on the item or item's packaging.

21. A method for determining if an item is a fraudulent item, the method comprising the steps of:

obtaining by radio means a first and second number from an RFID tag, wherein the first number is unalterable and unique or semi-unique and the second number is associated with the item;

electronically reading a third number;

utilizing a public-key cryptographic process and the first and second numbers to cryptographically decide whether the third number is a public-key signature of a combination of the first and second numbers; and

determining authenticity of the item based on the result of the decision.

22. The method according to claim 21 further comprising the step of electronically determining whether the RFID tag is an anti-forgery RFID tag.

23. The method according to claim 21, further comprising electronically determining whether a specific physical feature or a behavioral feature of the RFID tag matches that of an anti-forgery RFID tag.

24. The method according to claim 21 further comprising the step of verifying that the second number is associated with the item.

25. The method according to claim 24, wherein the verification is performed electronically using an optical scanner.

26. The method according to claim 21 further comprising the step of electronically determining whether the second number is an Electronic Product Code (EPC) of the item.

27. The method according to claim 21, wherein the reading is performed by a bar code scanner.

28. A method according to claim 6, wherein the second number is associated with the product.

29. A method according to claim 1, wherein:

the first number contains a third and fourth number,

the third number is concatenated with, and contains different information than, the fourth number,

the third number includes product information of the item,

the public-key cryptographic process is used with the third and fourth numbers, and

only if the public-key cryptographic process cryptographically decides that the second number is a public-key signature of the third and fourth numbers is the product determined to be authentic.

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

None.